UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/025,541	12/26/2001	Robert Edward Moore	01.133.01	8301

7590 06/13/2006

Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120

EXAMINER	
BLUDAU, BRANDON S	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 06/13/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Supplemental **Notice of Allowability**	Application No. 10/025,541	Applicant(s) MOORE ET AL.	
	Examiner Brandon S. Bludau	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *phone conversation on May 24, 2006*.

2. ☒ The allowed claim(s) is/are *1,4,5,7-11,14,15,17-21,24,25 and 29-38*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

This action is in reply to a request made by the Applicant on May 24th, 2006 by e-mail and phone conversation to amend Claim 33 after an issue of Allowance mailed by the Office on April 20th, 2006.

It was determined by the examiner that the request did not involve any new issues in the prosecution and is being allowed for entry.

EXAMINER'S AMENDMENT

Please enter the amended claim immediately below to the claim set following.

The amended claim 33 is as follows:

33. (Currently Amended) [[A computer program product as claimed in claim 1,]] A computer program product embodied on a computer readable medium for controlling a computer to identify a computer file as potentially containing malware, said computer program product comprising:

searching code to search within said computer file for text data containing one or more target words that match at least one of a word or a characteristic of a word within a predetermined word library, wherein said target words include a phonetic equivalent thereof such that said searching code further searches within said computer file for text data containing one or more phonetic equivalents of said target words that match a phonetic equivalent of a word within said predetermined word library;

context identifying code to identify a context within said computer file of said one or more target words;

context identifying code to identify a context within said computer file of said one or more target words; and

file identifying code to identify said computer file as potentially containing malware, if said context matches one or a predetermined set of contexts;

wherein said predetermined word library includes one or more of:

words that are names associated with known malware authors;

word format characteristics that are indicative of words being part of a message embedded within said computer file by a malware author; and

word suffix characteristics that are indicative of words being part of a message embedded within said computer file by a malware author;

wherein said predetermined set of contexts includes one or more of:

within a script portion of a webpage;

within a comment of a webpage; and

within a predetermined proximity to another target word.

The examiner also includes a clean copy of all claims in their allowable form provided below.

---

1. A computer program product embodied on a computer readable medium for controlling a computer to identify a computer file as potentially containing malware, said computer program product comprising:

searching code to search within said computer file for text data containing one or more target words that match at least one of a word or a characteristic of a word within a predetermined word library;

context identifying code to identify a context within said computer file of said one or more target words; and

file identifying code to identify said computer file as potentially containing malware, if said context matches one or a predetermined set of contexts;

wherein said predetermined word library includes one or more of:

words that are names associated with known malware authors;

word format characteristics that are indicative of words being part of a message embedded within said computer file by a malware author; and

word suffix characteristics that are indicative of words being part of a message embedded within said computer file by a malware author;

wherein said predetermined set of contexts includes one or more of:

within a script portion of a webpage;

within a comment of a webpage; and

within a predetermined proximity to another target word;

wherein, if said computer file is identified as potentially containing malware, then trigger thresholds associated with one or more other malware identifying processes applied to said computer file are adjusted to be more sensitive.

2. (Cancelled)

3. (Cancelled)

4. A computer program product as claimed in claim 1, wherein as a result of the one or more other malware identifying processes, identified malware is acted upon with one or more malware found actions.

5. A computer program product as claimed in claim 4, wherein said malware found actions include one or more of:

quarantining said computer file;

deleting said computer file;

issuing a warning message concerning said computer file; and

deleting a portion of said computer file suspect of containing malware.

6. (Cancelled)

7. A computer program product as claimed in claim 1, wherein if said computer file is identified as potentially containing malware, then a trigger threshold associated with a heuristic malware identifying process applied to said computer file is set to a more sensitive level.

8. A computer program product as claimed in claim 1, wherein all of said computer file is searched for said target words.

9. A computer program product as claimed in claim 1, wherein only those portions of said computer file matching said predetermined set of contexts are searched for said target words.

10. A computer program product as claimed in claim 1, wherein said malware comprises one or more of a computer virus, a worm and a Trojan.

11. A method of identifying a computer file as potentially containing malware, said method comprising the step of:

searching within said computer file for text data containing one or more target words that match at least one of a word or a characteristic of a word within a predetermined word library;

identifying a context within said computer file of said one or more target words; and

if said context matches one or a predetermined set of contexts, then identifying said computer file as potentially containing malware;

wherein said predetermined word library includes one or more of:

words that are names associated with known malware authors;

word format characteristics that are indicative of words being part of a message embedded within said computer file by a malware author; and

word suffix characteristics that are indicative of words being part of a message embedded within said computer file by a malware author;

wherein said predetermined set of contexts includes one or more of:

within a script portion of a webpage;

within a comment of a webpage; and

within a predetermined proximity to another target word;

wherein, if said computer file is identified as potentially containing malware, then trigger thresholds associated with one or more other malware identifying processes applied to said computer file are adjusted to be more sensitive.

12. (Cancelled)

13. (Cancelled)

14. A method as claimed in claim 11, wherein as a result of the one or more other malware identifying processes, identified malware is acted upon with one or more malware found actions.

15. A method as claimed in claim 14, wherein said malware found actions include one or more of:

quarantining said computer file;

deleting said computer file;

issuing a warning message concerning said computer file; and

deleting a portion of said computer file suspect of containing malware.

16. (Cancelled)

17. A method as claimed in claim 11, wherein if said computer file is identified as potentially containing malware, then a trigger threshold associated with a heuristic malware identifying process applied to said computer file is set to a more sensitive level.

18. A method as claimed in claim 11, wherein all of said computer file is searched for said target words.

19. A method as claimed in claim 11, wherein only those portions of said computer file matching said predetermined set of contexts are searched for said target words.

20. A method as claimed in claim 11, wherein said malware comprises one or more of a computer virus, a worm and a Trojan.

21. Apparatus including a program embodied on a computer readable medium for identifying a computer file as potentially containing malware, said apparatus comprising:

searching logic to search within said computer file for text data containing one or more target words that match at least one of a word or a characteristic of a word within a predetermined word library;

context identifying logic to identify a context within said computer file of said one or more target words; and

file identifying logic to identify said computer file as potentially containing malware, if said context matches one or a predetermined set of contexts;

wherein said predetermined word library includes one or more of:

words that are names associated with known malware authors;

word format characteristics that are indicative of words being part of a message embedded within said computer file by a malware author; and

word suffix characteristics that are indicative of words being part of a message embedded within said computer file by a malware author;

wherein said predetermined set of contexts includes one or more of:

within a script portion of a webpage;

within a comment of a webpage; and

within a predetermined proximity to another target word;

wherein, if said computer file is identified as potentially containing malware, then trigger thresholds associated with one or more other malware identifying processes applied to said computer file are adjusted to be more sensitive.

22. (Cancelled)

23. (Cancelled)

24. Apparatus as claimed in claim 21, wherein as a result of the one or more other malware identifying processes, identified malware is acted upon with one or more malware found actions.

25. Apparatus as claimed in claim 24, wherein said malware found actions include one or more of:

quarantining said computer file;
deleting said computer file;
issuing a warning message concerning said computer file; and
deleting a portion of said computer file suspect of containing malware.

26. (Cancelled)

27. Apparatus as claimed in claim 21, wherein if said computer file is identified as potentially containing malware, then a trigger threshold associated with a heuristic malware identifying process applied to said computer file is set to a more sensitive level.

28. Apparatus as claimed in claim 21, wherein all of said computer file is searched for said target words.

29. Apparatus as claimed in claim 21, wherein only those portions of said computer file matching said predetermined set of contexts are searched for said target words.

30. Apparatus as claimed in claim 21, wherein said malware comprises one or more of a computer virus, a worm and a Trojan.

31. A computer program product as claimed in claim 1, wherein said predetermined word library includes: words that are names associated with known malware authors; words that are indicative of being part of a message embedded within said computer file by a malware author; word format characteristics that are indicative of words being part of a message embedded within said computer file by a malware author; and word suffix characteristics that are indicative of words being part of a message embedded within said computer file by a malware author.

32. A computer program product as claimed in claim 1, wherein said predetermined set of contexts includes: within a script portion of a webpage; within a comment of a webpage; within executable code; and within a predetermined proximity to another target word.

33. A computer program product embodied on a computer readable medium for controlling a computer to identify a computer file as potentially containing malware, said computer program product comprising:

searching code to search within said computer file for text data containing one or more target words that match at least one of a word or a characteristic of a word within a predetermined word library, wherein said target words include a phonetic equivalent thereof such that said searching code further searches within said computer file for text data containing one or more phonetic equivalents of said target words that match a phonetic equivalent of a word within said predetermined word library;

context identifying code to identify a context within said computer file of said one or more target words;

context identifying code to identify a context within said computer file of said one or more target words; and

file identifying code to identify said computer file as potentially containing malware, if said context matches one or a predetermined set of contexts;

wherein said predetermined word library includes one or more of:

words that are names associated with known malware authors;

word format characteristics that are indicative of words being part of a message embedded within said computer file by a malware author; and

word suffix characteristics that are indicative of words being part of a message embedded within said computer file by a malware author;

wherein said predetermined set of contexts includes one or more of:

within a script portion of a webpage;

within a comment of a webpage; and

within a predetermined proximity to another target word.

34. A computer program product as claimed in claim 1, wherein said computer file identified as potentially containing malware is prevented from being transmitted outward from a mail server and is further analyzed when being transmitted inward to said mail server.

35. A computer program product as claimed in claim 7, wherein said heuristic malware identifying process is set to a more sensitive level by reducing a suspicious activities score required to trigger identification of said computer file as containing malware.

36. A computer program product embodied on a computer readable medium for controlling a computer to identify a computer file as potentially containing malware, said computer program product comprising:

searching code to search within said computer file for text data containing one or more target words that match at least one of a word or a characteristic of a word within a predetermined word library;

context identifying code to identify a context within said computer file of said one or more target words; and

file identifying code to identify said computer file as potentially containing malware, if said context matches one or a predetermined set of contexts;

wherein said predetermined word library includes one or more of:

words that are names associated with known malware authors;

word format characteristics that are indicative of words being part of a message embedded within said computer file by a malware author; and

word suffix characteristics that are indicative of words being part of a message embedded within said computer file by a malware author;

wherein said predetermined set of contexts includes one or more of:

within a script portion of a webpage;

within a comment of a webpage; and

within a predetermined proximity to another target word;

wherein if said computer file is identified as potentially containing malware, then a trigger threshold associated with a heuristic malware identifying process applied to said computer file is set to a more sensitive level.

37. A method of identifying a computer file as potentially containing malware, said method comprising the step of:

searching within said computer file for text data containing one or more target words that match at least one of a word or a characteristic of a word within a predetermined word library;

identifying a context within said computer file of said one or more target words; and

if said context matches one or a predetermined set of contexts, then identifying said computer file as potentially containing malware;

wherein said predetermined word library includes one or more of:

words that are names associated with known malware authors;

word format characteristics that are indicative of words being part of a message embedded within said computer file by a malware author; and

word suffix characteristics that are indicative of words being part of a message embedded within said computer file by a malware author;

wherein said predetermined set of contexts includes one or more of:

within a script portion of a webpage;

within a comment of a webpage; and

within a predetermined proximity to another target word;

wherein if said computer file is identified as potentially containing malware, then a trigger threshold associated with a heuristic malware identifying process applied to said computer file is set to a more sensitive level.

38. Apparatus including a program embodied on a computer readable medium for identifying a computer file as potentially containing malware, said apparatus comprising:

searching logic to search within said computer file for text data containing one or more target words that match at least one of a word or a characteristic of a word within a predetermined word library;

context identifying logic to identify a context within said computer file of said one or more target words; and

file identifying logic to identify said computer file as potentially containing malware, if said context matches one or a predetermined set of contexts;

wherein said predetermined word library includes one or more of:

words that are names associated with known malware authors;

word format characteristics that are indicative of words being part of a message embedded within said computer file by a malware author; and

word suffix characteristics that are indicative of words being part of a message embedded within said computer file by a malware author;

wherein said predetermined set of contexts includes one or more of:

within a script portion of a webpage;

within a comment of a webpage; and

within a predetermined proximity to another target word;

wherein if said computer file is identified as potentially containing malware, then a trigger threshold associated with a heuristic malware identifying process applied to said computer file is set to a more sensitive level.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Bludau whose telephone number is 571-272-3722. The examiner can normally be reached on Monday -Friday 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Brandon S Bludau
Examiner
Art Unit 2132
BB

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100